DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of the Army organizational name (APMS Sub Organization name).

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command (FMWRC)

2. Name of Information Technology (IT) System (APMS System name).

Personal Development System (PDS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

589

5. IT Investment (OMB Circular A-1 1) Unique Identifier (if applicable)

NA

6. Privacy Act System of Records Notice Identifier (if applicable).

A0215 CFSC, General Morale, Welfare, Recreation and Entertainment Records (October 17, 2001, 66 FR 52750).

The system notice will be updated specific to this data collection.

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

NA

8. Type of authority to collect information (statutory or otherwise).

5 USC 3111, Acceptance of volunteer service
10 U.S.C. 3013, Secretary of the Army;
10 USC 1588, Authority to accept certain voluntary services
26 U.S.C. 6041, Information at Source;
Army Regulation 215-1, Morale Welfare, and Recreation Activities and Non-appropriated Fund Instrumentalities;
DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR);

DoD Instruction 1015.10, Program for Military Morale, Welfare, and Recreation (MWR); E.O. 9397 (SSN)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup).

To establish an individual's eligibility for Army Community Services (ACS), to verify ACS personnel access to the system, to build conference rosters and courses and to produce travel orders for attendees. These conferences are conducted to execute various Army programs.

The goals of the Personal Development System (PDS) are to: enhance the readiness of Soldiers and units, improve Soldier performance, and retain Soldiers and families within the Army system. PDS is supported by a web-based application that resides on the MyArmyLifeToo.com portal. It is the public face of HQDA Family Programs Directorate and serves as the official portal to Army Families worldwide. The application allows users to improve their life skills, enhance their self-reliance and understanding of the Army, gain access to resources for employment and career development, build connections with others throughout the military, manage their personal accomplishments, and grow as contributors and leaders within the Army community. It is owned by HQDA Family Programs Directorate and operated by DefenseWeb Technologies, Inc. The various components of the web system are the e-Learning Management and Conference Modules. All systems are backed up on a nightly and weekly schedule.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).

The personally identifiable information collected for site registration to take an online course or subscribe to the Family News (a monthly listserv) include: name, address, military community, email, and development of a username and password. Individuals will enter their own information into the site to register and/or subscribe.

The personally identifiable information collected for conference registration and volunteer registration include: name, SSN, email, home and work address, rank and/or title, Federal Employee status, emergency contact, military community affiliation, region, gender, marital status, supervisor name, supervisor phone, supervisor e-mail, Soldier/Spouse/Youth/Parent status for Active/Guard or Reserve, Anti-Terrorism training date, Group Affiliation (Civilian, Retiree, Soldier, Dual Military, Parent, Better Opportunities for Single Soldiers (BOSS), Widow, Widower and Wounded Warrior). Conference attendees enter their information on their own and it is verified by a Regional level ACS Manager and re-verified by HQDA ACS Program Managers. Volunteer Registration does not ask for emergency contact or parent information. Conference Registration forms can vary with the type of information collected. For

example, an AIFSN Basic Conference does not request emergency contact, marital status or parent names in the registration form.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

In most cases, site and conference registrants enter information individually via the web; however, conference registrants may register by paper or telephone, and administrators will enter data into the system. Likewise, volunteers may choose to interact with Army Volunteer Coordinators in person to register, apply for positions, and record hours of service, rather than interact with the online system.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

These conferences are conducted to execute various DA programs according to Army Regulations 600-20 and 608-1. Information in identifiable form is collected to establish an individual's eligibility for ACS Services, to verify ACS personnel access to the system, to build conference rosters and courses and to produce travel orders for attendees.

Volunteer positions are managed similar to other jobs in that the social security number is used to track a volunteer's service across all installations.

13. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation.

14. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies).

Some information is shared with other conference attendees. Information is provided to Army law enforcement in order to verify suitability for attendance. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

15. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Before any PII is collected, individuals are provided a privacy act advisory statement. Individuals choose to enter their own information into the system. Army subject matter experts and other participants, who attend on orders, do not have the option to refuse to provide PII. Voluntary conference registrants may choose not to use the MyArmyLifeToo system online conference registration. If they choose not to use the online registration, they will need to coordinate directly with the ACS Staff managers. Likewise, should volunteers choose not to use the online Volunteer Management Information System to register, apply for positions or track hours of service, they can visit the local ACS office to perform those tasks in person.

16. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

A Privacy Act Statement is displayed when a user logs into the system. An individual who objects to providing information will be denied access to the online courses, subscriptions or conference attendance. Also, a link which displays the Privacy Act Statement is provided at the top of both the conference registration form and the volunteer registration form.

17. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

The data is stored within a secure datacenter on a secure Army Installation with all protections afforded by Army and Defense Information System Agency (DISA) security infrastructure. The datacenter has passed the required security measures tests required for Information Assurance System Accreditation and has a full Authority to Operate. Web, database and application servers are clustered for redundancy, however, no datacenter redundancy is currently provided.

All ACS Personnel accessing government computer information are required to undergo and receive at a minimum favorable local, state and national security checks. The users include Federal Civil Service personnel and authorized contractors of ACS that have a need to know in order to perform official government duties. Both contractor and government employees may have access requirements and are limited to specific or general information in the computing environment; thus, certain types of data are restricted to only certain access levels within the system. Each user has a unique username for the system. If the user has an access level to retrieve data, their username and password will allow them to view it. These access levels are assigned by System Administrators to authorized personnel on an "as needed" basis. Data search results in the system are for one record, as opposed to searching through multiple data records. All data is filtered by installations and can not be searched by users not authorized for the particular installation the data is stored under. As personal

information is entered, it is passed to the web browser via a HTTPS encrypted connection and stored in an encrypted database.

Information is made available to users based on their roles through the application or Enterprise server. Each authorized user must enter an appropriate User/Identification and Password before being authorized access to the resources. Various checks are in place to ensure accuracy such as data field validation, mandatory data elements and approval chains for conference registration.

There is weekly monitoring and immediate disabling of accounts with easily guessed passwords, daily notification of inactive accounts, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's).

18. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A system notice exists currently. Either the existing system notice will be amended to be more descriptive of this business practice or an entirely new system notice will be developed.

19. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risk is mitigated by consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies.

20. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The PDS program privacy data is for official use only. The PIA may be published in its entirety.